Shark, Software S1019 | MITRE ATT&CK®

Archived: 2026-04-05 15:32:35 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Shark has the ability to use HTTP in C2 communications.[1][2]
		.004	Application Layer Protocol: DNS	Shark can use DNS in C2 communications.[1][2]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Shark has the ability to use `CMD` to execute commands.[1][2]
Enterprise	T1005		Data from Local System	Shark can upload files to its C2.[1][2]
Enterprise	T1074		Data Staged	Shark has stored information in folders named `U1` and `U2` prior to exfiltration.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Shark can extract and decrypt downloaded .zip files.[1]
Enterprise	T1568	.002	Dynamic Resolution: Domain Generation Algorithms	Shark can send DNS C2 communications using a unique domain generation algorithm.[1][2]
Enterprise	T1041		Exfiltration Over C2 Channel	Shark has the ability to upload files from the compromised host over a DNS or HTTP C2 channel.[1]
Enterprise	T1008		Fallback Channels	Shark can update its configuration to use a different C2 server.[1]

Domain	ID		Name	Use
Enterprise	T1070	.004	Indicator Removal: File Deletion	Shark can delete files downloaded to the compromised host.[1]
Enterprise	T1105		Ingress Tool Transfer	Shark can download additional files from its C2 via HTTP or DNS.[1][2]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	Shark binaries have been named `audioddg.pdb` and `Winlangdb.pdb` in order to appear legitimate.[1]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	Shark can use encrypted and encoded files for C2 configuration.[1][2]
Enterprise	T1012		Query Registry	Shark can query `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography MachineGuid` to retrieve the machine GUID.[2]
Enterprise	T1029		Scheduled Transfer	Shark can pause C2 communications for a specified time.[1]
Enterprise	T1082		System Information Discovery	Shark can collect the GUID of a targeted machine.[1][2]
Enterprise	T1497	.001	Virtualization/Sandbox Evasion: System Checks	Shark can stop execution if the screen width of the targeted machine is not over 600 pixels.[1]
